The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

07/01/2014

SUBJECT:

Multiple Vulnerabilities in Apple iOS

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Apple's mobile operating system, iOS. These vulnerabilities can be exploited by an attacker having physical access to the device, or if the user visits a specially crafted webpage. Successful exploitation could result in an attacker executing arbitrary code, cause denial-of-service conditions, gain unauthorized access, acquire sensitive information, bypass security restrictions, and perform other unauthorized actions.

THREAT INTELLIGENCE

Due to the trivial nature of these vulnerabilities, there is not any known proof-of-concept code available.

SYSTEM AFFECTED:

· Apple iOS Prior to 7.1.2

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Nine vulnerabilities have been reported in Apple iOS. Details of the vulnerabilities are as follows:

- A spoofing vulnerability when handling a specially crafted website. [CVE-2014-1345]
- A security weakness exists due to data protection being disabled. [CVE-2014-1348]
- A use-after-free error when handling a specially crafted website. [CVE-2014-1349]
- A security-bypass vulnerability when handling "Find My iPhone". [CVE-2014-1350]
- A security-bypass vulnerability exists due to a failure to restrict access to view all contacts. [CVE-2014-1351]
- A security-bypass vulnerability exists due to a failure to properly enforce a maximum number of failed passcode attempts. [CVE-2014-1352]
- A security-bypass vulnerability exists due to improper state management in Airplane Mode [CVE-2014-1353]
- A remote-code execution when handling a specially crafted XMB file. [CVE-2014-1354]
- A security-bypass vulnerability due to a failure to properly check during device activation. [CVE-2014-1360]

Successful exploitation could result in an attacker executing arbitrary code, cause denial-of-service conditions, gain unauthorized access, acquire sensitive information, bypass security restrictions, and perform other unauthorized actions.

RECOMMENDATIONS:

The following actions should be taken:

- Update Apple iOS to the most current version, 7.1.2.
- Use safe web browsing techniques to avoid visiting specially crafted webpages.
- Avoid leaving Apple iOS devices unattended.

REFERENCES:

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1345

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1348

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1349

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1350

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1351

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1352

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1353

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1354

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1360

SecurityFocus:

http://www.securityfocus.com/bid/68276